QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Thao Thai (CA Bar No. 324672)
thaothai@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

William A. Burck (admitted *pro hac vice*)
williamburck@quinnemanuel.com
Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
1300 I. Street, N.W., Suite 900
Washington, D.C. 20005
Telephone: 202-538-8000
Facsimile: 202-538-8100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Jomaire A. Crawford (admitted *pro hac vice*)
jomairecrawford@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Attorneys for Defendant Google LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

CHASOM BROWN, MARIA NGUYEN, WILLIAM BYATT, JEREMY DAVIS, and CHRISTOPHER CASTILLO, individually and on behalf of all similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 5:20-cv-03664-LHK

GOOGLE'S REPLY IN SUPPORT OF MOTION TO DISMISS FIRST AMENDED COMPLAINT

The Honorable Lucy H. Koh
Courtroom 8 – 4th Floor
Date: February 25, 2021
Time: 1:30 p.m.

Amended Complaint Filed: Sept. 21, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutory Authorities

INTRODUCTION

The dispositive facts remain undisputed. Plaintiffs admit that: (1) they consented to Google's Privacy Policy; and (2) the Privacy Policy expressly disclosed that Google receives the categories of data at issue ("Data") from websites that use its third-party web services, including Ad Manager and Analytics. Indeed, Plaintiffs acknowledge it is "common knowledge" that Google receives such Data from "users who are not in 'private browsing mode.'" AC ¶ 163. Yet Plaintiffs contend that, in the same Privacy Policy that disclosed Google's receipt of the Data, Google also represented that using private browsing mode would *prevent* Google from receiving the Data. It did not. And any misunderstanding Plaintiffs allege they had about the Privacy Policy's disclosures would have been definitively resolved by the *full-page* Incognito Notice—shown to Plaintiffs *every time* they used Chrome's private browsing mode—which makes clear that "browse privately" means "*other people who use this device won't see your activity*," but "[y]our activity may still be visible to," among others, "[w]ebsites you visit," and "[y]our internet service provider." AC ¶ 52 (emphasis added).

Plaintiffs try in vain to dodge the Incognito Notice by essentially arguing that "Now you can browse privately, and *other people who use this device won't see your activity*" means "Now you can browse privately and *Google won't see your activity*." *See* Opp. 9. But their argument is implausible on its face and should be rejected out of hand.

Plaintiffs also assert (at 1) that "Google repeatedly (and falsely) assured Plaintiffs that they … could 'browse the web privately' without Google 'linking any activity to you.'" There is nothing false about Google's statements. As the disclosures Plaintiffs cite make clear, "browsing in private usually means" that cookies may still be set during a private browsing session but they are "deleted *after you close your private browsing window or tab*." Ex. 18 (cited at AC ¶¶ 47-48) (emphasis added); *see also* Ex. 17, at 7 (Chrome Privacy Notice stating that cookies set during Incognito session will "be stored and transmitted until you close the Incognito window"). This is how Incognito mode works. As a result, when Plaintiffs browse the web in Incognito mode while logged out of their Google accounts—as they allege (AC ¶ 192)—any Data Google receives from that browsing session ultimately is not linked to them or their accounts. The AC does not plausibly allege otherwise, and therefore Plaintiffs' invasion of privacy claims fail as a matter of law.

All claims should be dismissed because Plaintiffs consented to the Privacy Policy—which disclosed that Google receives the Data—and nothing in Google's disclosures negates their consent. Plaintiffs' claims should also be dismissed for the independent reasons explained in the Motion and below.

ARGUMENT

I. PLAINTIFFS AND THE WEBSITES CONSENTED TO GOOGLE'S RECEIPT OF THE DATA[1]

A. Plaintiffs Consented to Google's Receipt of the Data

As demonstrated above and in the Motion, there is no dispute that Plaintiffs consented to the Privacy Policy when they signed up for their Google accounts, and that the Privacy Policy disclosed Google's receipt of the Data at issue from its web services, like Analytics and Ad Manager.

Plaintiffs misleadingly quote excerpts from Google's Privacy Policy (and support pages) to argue that "Google's Privacy Policy states that private browsing mode … *prevents* Google from collecting the data it typically collects by way of the services it provides to websites." Opp. 6-7 (emphasis added). But none of the statements on which Plaintiffs rely supports their argument:

> "You can use ***our services*** in a variety of ways to manage your privacy. For example … [y]ou can [] choose to browse the web privately using Chrome in Incognito mode…."
>
> "And across ***our services***, you can adjust your privacy settings to control and how your information is used."

Opp. 7 (quoting Ex. 8 (3/25/18 Privacy Policy), at 1) (emphasis added by Plaintiffs). These are general statements from a paragraph discussing the *many* privacy settings available on Google's *many* services to manage privacy in a *variety* of ways. Indeed, the topic sentence is: "You can use

[1] Plaintiffs argument (at 6) that consent cannot defeat their claims at the pleading stage is meritless. *See Garcia v. Enter. Holdings, Inc.*, 78 F. Supp. 3d 1125, 1135-36 (N.D. Cal. 2015) ("lack of consent is an express element of a [CIPA] claim" and "properly challenged … through [a] motion to dismiss"); *Shefts v. Petrakis*, 2011 WL 5930469, at *7 n. 10 (C.D. Ill. Nov. 29, 2011) (consent is a statutory exception under the ECPA and thus "lack of authorization [or consent] is an element Plaintiff[s] must prove"); *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 790 n. 9 (N.D. Cal. 2019) ("the Court must dismiss the claims regardless of whether consent is an element or a defense" where "the allegations in the complaint and any judicially noticeable materials definitively establish that the plaintiffs consented to the conduct") (citing *Rivera v. Peri & Sons Farms, Inc.*, 735 F.3d 892, 902 (9th Cir. 2013)).

our services in a variety of ways to manage your privacy," which is supported by examples about the many different privacy settings that Google offers "across [its many] services." Neither statement suggests that using Incognito mode prevents Google from receiving the Data at issue.

> "You're in control of what information you share with Google when you search. ***To browse the web privately, you can use private browsing...***"

Opp. 7 (quoting AC ¶ 42, in turn quoting Ex. 18) (emphasis added by Plaintiffs)). This quote is excerpted from a support page titled "Search & browse privately." Plaintiffs do not allege they reviewed it, but even if they had, the page is not inconsistent with the Privacy Policy and Incognito Notice. The page describes a number of tools available to users to control information they "share with Google when [they] search." Plaintiffs misleadingly omit most of these by ellipses, but the tools include "us[ing] private browsing, sign[ing] out of your account, chang[ing] you custom results settings, or delet[ing] past activity." Ex. 18, at 1.

Nowhere does the page suggest that any of these options (or a combination of them) prevents Google from receiving the Data at issue here. To the contrary, the *next sentence* (omitted by Plaintiffs) makes clear that private browsing allows users "to search the web *without saving your search activity* to your [Google] account." *Id.* (emphasis added). And the subsequent "How private browsing works" section (Plaintiffs omit that too) contains four plain language bullets explaining the practical effects of private browsing, including that "[t]he searches you do or sites you visit won't be saved *to your device or browsing history*." *Id.* Importantly, one of the bullets explains that "you might see search results and suggestions based on … other searches you've done *during* your current private browsing session," *id.*, which indicates that Google receives Data during the session. The page makes clear, however, that the cookies linking that Data to the user's browser "are deleted after you close your private browsing window or tab." *Id.*

> "Chrome won't save … [y]our browsing history [and] [c]ookies and site data."

Opp. 7 (quoting AC ¶ 52 (screenshot of Incognito Notice)). Plaintiffs ignore that the Incognito Notice in which this quote appears states, in the very first sentence, that "browse privately" here means "*other people who use this device* won't see your activity." *See* AC ¶ 52 (emphasis added). The statement that "*Chrome* won't save … [y]our browsing history [and] [c]ookies and site data" is

limited by its terms: *Chrome* (*i.e.*, the browser) will not save such information within the browser to prevent "other people who use this device" from seeing it. The sentence does not speak to Google's receipt of the Data from third-party websites that use Analytics and Ad Manager services.

> "Your activity might still be visible to: the websites you visit, your employer or school, or your internet service provider."

Opp. 7 (quoting Incognito Notice at AC ¶ 52). The Incognito Notice is presented precisely to ensure users understand what Incognito mode means, and that it does not make a user's browsing activity "invisible." Activity is kept private from "other people who use this device" but "might still be visible" to a number of third parties, including websites that use Google's third-party services.

Plaintiffs' criticism (at 8-9) that the Incognito Notice itself does not specifically "disclose that 'Google' is one of the 'ads and resources' on websites that might be privy to private browsing communications," is meritless. The Privacy Policy, to which Plaintiffs admittedly consented, disclosed exactly that: "We … collect and store information when you interact with services we offer to our partners, such as advertising services or Google features *that may appear on other sites*." Ex. 1, at 4 (emphasis added); *see id.* at 2 ("We collect information about the services that you use and how you use them, like when you … *visit a website that uses our advertising services*") (emphasis added). Plaintiffs were thus on notice that their browsing activity would be visible to third-parties, including websites that, as Plaintiffs acknowledge (AC ¶ 163), routinely choose to share such information with service providers, *including Google*.

> "For example, we recently brought Incognito mode, the popular feature in Chrome that lets you browse the web without linking any activity to you, to YouTube."

Opp. 1, 3, 7 (citing AC ¶ 146 (quoting New York Times op-ed)). This quote is from an op-ed Google's CEO published in the New York Times (which Plaintiffs do not allege they read), and is entirely consistent with Google's disclosures that cookies linking Data from an Incognito session to a user's browser are deleted when the session is closed.[2]

[2] None of the other "numerous statements" Plaintiffs cite (Opp. 7 (citing AC ¶¶ 42, 146)) support their arguments. Rather, they are snippets from articles, blogs, or disclosures that Plaintiffs do not allege they read and which they misleadingly quote out of context.

As shown above, none of the statements Plaintiffs quote supports their assertion (at 6) that "Google's Privacy Policy states that private browsing mode (including Incognito mode) prevents Google from collecting the data it typically collects by way of the services it provides to websites." Accepting Plaintiffs' argument requires piling untenable inference upon inference from snippets of disclosures and support pages while ignoring the plain meaning of the statements in the context of the documents in which they appear.

Plaintiffs' reliance (at 8) on this Court's decision in *In re Google Inc.*, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013) (Koh, J.) ("*Gmail*"), cannot salvage their claims. The Court there held that Google's Privacy Policy did not "specifically mention the content of users' emails" among the data Google collects and thus "a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements." *Id.* at *14. Here, by contrast, the Privacy Policy specifically discloses that Google receives the Data at issue, and Plaintiffs do not contend otherwise.

B. The Websites Consented to Google's Receipt of the Data

The AC accurately alleges that websites install Google's Analytics and Ad Manager code *for the purpose of transmitting the Data to Google* to obtain Google's services. AC ¶¶ 64-68 (Analytics); *id.* ¶¶ 78-79 (Ad Manager). The only reasonable inference is that the websites consented to Google's receipt of the Data, and Plaintiffs' claim under the Wiretap Act—a "one party consent" statute—may be dismissed on this basis alone.

Plaintiffs contend (at 11) that, regardless of whether users are in private browsing mode, "websites could not have consented" to the transmission of the Data to Google because the duplicated GET requests Google allegedly "intercepted" are "*additional* message[s]" which the websites are "not directly part of" and which websites thus lack authority to share with Google. *Id.* But every "communication" requires at least two parties—a sender *and a recipient*. Under Plaintiffs' theory, the "additional messages" are between them and Google, making Google a party and exempt under § 2511(c)(2). As Plaintiffs know, however, the Ninth Circuit has held that web service providers that receive simultaneous duplicated GET requests are *not* parties to the alleged "communications." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020)

("*Facebook*"). Plaintiffs' theory thus creates a paradox: (1) the websites are not parties (and thus lack authority to consent) because the alleged "communications" are "additional messages" sent *directly* to Google; but (2) Google is not a party either because the Ninth Circuit said so in *Facebook*. *See id.* That would mean the user is the *only* party to the communications—and the only party that can provide consent under § 2511(2)(c)—which is illogical and inconsistent with the statute, which plainly contemplates that either the sender *or* the recipient(s) may provide consent to interception. *Id.* Simply put, there needs to be a recipient of the "communications" that can consent to the alleged interception, and the only two possibilities here are the websites or Google.

Implicit in the Ninth Circuit's holding in *Facebook* is that, when a GET request is simultaneously duplicated and sent directly to a third-party service provider, the "communication" remains between the user and the website. It follows that websites are parties to such communications and *can*—and necessarily *do*—consent to the provider's "interception" of them by choosing to install the provider's code to send the Data directly to the provider so that the websites can obtain the provider's services.[3]

Plaintiffs' alternative argument (at 11) that, even if the websites have the authority to consent to Google's receipt of the Data, the websites did not consent to receipt if "*users enabled private browsing mode*," is similarly meritless. Plaintiffs cite no authority holding that such specific consent is required, and their reliance on *Gmail* is misplaced. The Court there held that users consented to Google's analysis of emails "to exclude objectionable content, such as sexual material" but not "for the purposes of creating user profiles or providing targeted advertising." 2013 WL 5423918, at *12. Here, by contrast, it is clear that the websites consented to Google's receipt of the Data *for the purpose of* obtaining Google's advertising and analytics services, and Plaintiffs do not allege that

[3] Plaintiffs' theory should also be rejected because it posits that websites can consent to allowing their service providers to "intercept" the Data if it is sent *from the websites to the providers*, but not if the websites use code that sends the exact same Data *from the user's browser to the provider directly* (a common practice)—even though the end result (the provider receives the Data) is identical. Plaintiffs' argument thus challenges the *method* of the alleged "interception," which is irrelevant to the issue at hand—*i.e.*, whether "one of the parties to the communication has given prior *consent* to [the] interception." 18 U.S.C. § 2511(2)(c) (emphasis added).

Google used the Data other than to provide these services.[4] Nor do Plaintiffs plausibly allege that websites consented only for non-private browsing mode users.

C. Plaintiffs Fail to Establish That Google Intended to Commit a Crime or Tort

Plaintiffs' assertion (at 12-15) that consent is no defense because Google allegedly intercepted the Data for a criminal or tortious purpose is also baseless. Plaintiffs fail to "plead sufficient facts to support an inference that [Google] intercepted the communication *for the purpose of a tortious or criminal act* that is independent of the intentional act of recording." *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010) (emphasis added); *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1278 (C.D. Cal. 2001) ("the bare allegation [of a tortious purpose] mirroring the statutory language is insufficient to survive a Rule 12(b)(6) motion to dismiss.").

"Section 2511(2)(d)'s legislative history and case law make clear that the 'criminal' or 'tortious' purpose requirement is to be construed narrowly." *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 515 (S.D.N.Y. 2001). Plaintiffs must allege either the "primary motivation or a determining factor in the interceptor's actions has been *to injure plaintiffs tortiously*." *In re Google Inc., Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014) (quotations and citations omitted; emphasis added). The exception applies only "[w]here the [interception] is legal, but is done for the purpose of facilitating some further impropriety, such as blackmail …" *Sussman v. Am. Broad. Companies, Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999).

The AC does not come close to meeting this standard. Plaintiffs argue (at 12-13) that "Google's [criminal or tortious] 'purpose' was to associate data from the intercepted private browsing communications with preexisting user profiles, enriching those profiles; to sell these profiles to advertisers; and to send targeted advertisements, based on the intercepted communications." Even taken as true—they are not—these alleged purposes fall far short of

[4] Plaintiffs' argument (at 12) that Google Analytics' beta "Consent Mode" constitutes an "admission" that Google received Data from the websites without their consent is specious. Consent Mode, which is in development, aims to provide additional, improved means for websites to record consent directly from *all* their users (*i.e.*, not merely Google account holders, like Plaintiffs, who admittedly were given notice of Google's Privacy Policy). Google's development of Consent Mode thus is not an "admission" that Google receives the Data without the websites' consent.

criminal or tortious. *See Doubleclick*, 154 F. Supp. 2d at 519 (the crime-tort exception does not apply where the interceptor's "purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money"); *Cohen v. Casper Sleep Inc.*, 2018 WL 3392877, at *3 (S.D.N.Y. July 12, 2018) (rejecting application of crime-tort exception because "collecting data to de-anonymize consumers was not Defendants' primary motivation" but "[r]ather … the means … to achieve their real purpose—marketing"). Here, the allegation is that Google's purpose was to make "profits," not to injure its users. *See* AC ¶¶ 113-38 ("Google profits from its surreptitious collection of user data.").

Nor is there merit to Plaintiffs' contention (at 13-15) that the crime-tort exception applies because Google's "subsequent acts" allegedly violated an FTC Consent Decree, the CCPA, the CDAFA, or constituted a privacy violation. Plaintiffs have not established such violations, but even if they had, the exception applies only if Google acted with "the purpose of committing [a] *criminal* or *tortious* act in violation of the *Constitution or laws* of the United States or of any State." 18 U.S.C. § 2511(2)(d) (emphasis added). The FTC consent decree is not law.[5] *United States v. ITT Cont'l Baking Co.*, 420 U.S. 223, 238 (1975) ("[A] consent decree or order is to be construed for enforcement purposes basically as a contract."). The CCPA is a civil statute that does not provide a private right of action (other than in the event of data breach) or for tort liability. *See United States v. Burke*, 504 U.S. 229, 234-35 (1992) ("an action for damages is an essential characteristic of every true tort"). And, as demonstrated *infra* at Sections II.C and D, Plaintiffs fail to establish that Google violated CDAFA/CCCL or invaded Plaintiffs' privacy, let alone that intentionally violating these laws and injuring Plaintiffs was Google's purpose in receiving the Data.

II. PLAINTIFFS' CLAIMS SHOULD BE DISMISSED FOR ADDITIONAL REASONS

A. Plaintiffs' Wiretap Act Claim (Count 1) Fails Because Google Received the Data in the Ordinary Course of Business

The lynchpin of this exception is the definition of "device," which exempts a "device" used "in the ordinary course of [] business." 18 U.S.C. § 2510(5)(a)(ii). This Court has held that the

[5] Plaintiffs' reliance (at 13) on *Hameed-Bolden v. Forever 21 Retail, Inc.*, 2018 WL 6802818 (C.D. Cal. Oct. 1, 2018) and *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783 (N.D. Cal. May 27, 2016), is misplaced because both cases involved UCL claims predicated on Federal Trade Commission Act violations.

exemption applies where there is a "nexus between the need to engage in the alleged interception and … the ability to provide the underlying service or good." *Gmail*, 2013 WL 5423918, at *11. Plaintiffs do not and cannot dispute that: (1) the alleged intercepting "device" is Google's Analytics and Ad Manager "code" that the websites "embed … into their existing webpage code" to transmit the Data "to Google's servers," AC ¶¶ 65-79; (2) the purpose of that code is to transmit the Data to Google to facilitate Google's provision of Analytics and Ad Manager services, *id.*; and (3) by definition Google could not provide those services without the Data. Thus, the "nexus" is present.

Plaintiffs try to analogize this case to *Gmail* by arguing that "Google's interception neither 'facilitates' nor is an 'instrumental part of' the *transmission from the user's computer to the website*." Opp. 15 (emphasis added). That is a red herring—Plaintiffs do not allege that the purpose of Google's code is to facilitate "transmission[s] from the user's computer to the website[s]." Rather, Plaintiffs allege that the purpose of Ad Manager code is to "cause[] the user's browser to display targeted Google advertisements" (AC ¶ 79), and the purpose of the Analytics code is to "provide[] data analytics" about "a Website's traffic" (*id.* ¶ 67). The AC leaves no doubt that the "interception" of the Data by way of Google's code is essential to its provision of these business services. In *Gmail*, by contrast, the Court emphasized that plaintiffs "allege[d] that [Google used] *separate* devices—[unrelated] to delivery of email—that intercept users' emails." 2013 WL 5423918, at *8. That is not the case here. The only "device" alleged is the Analytics and Ad Manager code that the AC admits is used to provide analytics and ad services.[6]

B. Plaintiffs' CIPA § 632 Claim (Count 2) Fails Because the Data Is Not a "Confidential Communication"[7]

CIPA § 632(c) excludes from the definition of "confidential communication" one "in which the parties to the communication may reasonably expect that the communication may be overheard

[6] Plaintiffs also argue (at 15) that the ordinary course of business exception does not apply because Google allegedly violated its own policies. This argument fails because, as shown above, Plaintiffs do not plausibly allege Google violated its policies.

[7] Plaintiffs' claims under CIPA §§ 631 and 632 should also be dismissed because all parties to the alleged "communications"—*i.e.*, plaintiffs and the websites—consented to Google's receipt of the Data. *See* Sections I.A and B, *supra.*

or recorded." California state and federal courts apply a "general rule" that "internet communications" are not confidential under § 632. *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, *3 (N.D. Cal. Oct. 23, 2019) (collecting cases); *see also* Mot. at 14-15 (citing cases). And, in *Revitch*, the court specifically applied this "general rule" to "browsing activity and form field entries" on a website that used embedded code to redirect data to a third-party service provider—*i.e.*, essentially the same facts alleged here. *See Revitch*, 2019 WL 5485330, at *1, 3.

Plaintiffs argue (at 17-18) that "the reasoning from [*Revitch*] does not apply" because the "communications" there involved "details about various items of clothing," whereas "Plaintiffs have alleged that Google intercepted their communications with thousands of different websites—including dating websites, political websites, and other highly sensitive and confidential websites." But the nature of the websites is irrelevant. Plaintiffs' claims are not limited to communications with dating and political sites; they purport to cover websites of any kind. The issue, then, is whether Plaintiffs had a reasonable expectation that their alleged "communications" with websites—*any websites*—would not be "overheard or recorded." Cal. Penal. Code § 632(c). The case law makes clear they did not because "internet communications" are routinely recorded and shared with service providers. *See* Mot. at 15 (citing cases).

Plaintiffs also argue that "they expected that their private browsing communications were not being overheard *by Google*." Opp. 17 (emphasis added). But the statute requires a reasonable expectation that the communications would not be "overheard or *recorded*" by *anyone*, including the websites. Plaintiffs admit they understood, at a minimum, that the *websites* would record the Data—*see* AC ¶¶ 63, 68 (acknowledging that alleged "communications" are sent to the "Website's server")—which defeats confidentiality under § 632.[8] In addition, given the Incognito Notice's disclosure that "[y]our activity might still be visible to … [y]our internet service provider," Plaintiffs were aware that their internet service providers may "overhear" their alleged communications with websites, which is independently fatal to their § 632 claim.

[8] Plaintiffs also argue that "Google's disclosures told its users that their private browsing communications … would 'not be saved' by Google." Opp. 17 (quoting AC ¶ 42). That is false. The cited disclosure states that, in Incognito mode, "browsing history" will not be saved *in the browser*.

Plaintiffs' reliance (at 16-17) on *Mirkarimi v. Nevada Prop. 1 LLC*, 2013 WL 3761530 (S.D. Cal. July 15, 2013) and *Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377 (2011), is misplaced. Both cases involved the recording of "telephone communications," which, unlike the internet communications at issue here, are oral, not routinely recorded and shared, and thus are not subject to the same "presumption" of non-confidentiality. *Cf. Gmail*, 2013 WL 5423918, at *23 ("Unlike phone conversations, email services are by their very nature recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else….").

C. Plaintiffs' CCCL Claim (Count 3) Does Not Satisfy the Statute's Requirements

Plaintiffs' California Computer Crime Law ("CCCL") claim fails at the outset because, as explained *supra* at I.A, Plaintiffs do not plausibly allege that Google took, copied or made use of the Data "without permission." Cal. Penal Code § 502(c)(2). Plaintiffs consented to the Privacy Policy, which disclosed the alleged data collection and uses.[9]

The claim also fails because Plaintiffs allege no more than violation of a "term of use," which is insufficient. *See Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010). Plaintiffs acknowledge that Google's collection and use of the Data to serve ads is both disclosed in the Privacy Policy and "common knowledge." AC ¶ 163. Yet, they argue (at 6) that Google's receipt of the Data was improper here because "Google's *Privacy Policy* states that private browsing mode … prevents Google from collecting the data."

Even if true, this cannot give rise to criminal liability. The Ninth Circuit has cautioned against "transforming otherwise innocuous behavior into [] crimes simply because a computer is involved," such as in cases, like this one, involving "permission skirmishes." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016). Before liability may be imposed under a criminal statute like the CCCL, Plaintiffs must allege facts showing the defendant intended to

[9] Plaintiffs' assertion (at 18) that Google acted without permission by "creating 'hidden' software code that 'sends secret instructions back to the user's browser, without alerting the user,'" is inconsistent with their allegations that (1) Google's allegedly "hidden" code is downloaded, installed, and used by "[o]ver 70% of … websites and publishers" on the Internet, AC ¶¶ 67-68, and (2) the "secret instructions" can be viewed by any user by simply clicking on "Developer Tools" in the Chrome browser, AC ¶ 86, 95. These allegations belie a criminal intent.

commit a crime by designing "software … in such a way to render ineffective any barriers the Plaintiffs must wish to use to prevent access to their information," *Brodsky v. Apple Inc.*, 2019 WL 4141936, at *9 (N.D. Cal. Aug. 30, 2019) (Koh, J.), or accessing data after receiving an "individualized cease-and-desist letter," and switching IP addresses to "circumvent IP barriers," *Power Ventures*, 844 F.3d at 1068-69.

Here, Plaintiffs do not allege that Google's Analytics or Ad Manager code can *determine* when a user is in private browsing mode, which belies their allegation that Google understood it was acting without permission. Nor do Plaintiffs plausibly allege that Google designed the code to render private browsing mode "ineffective." Rather, all Plaintiffs allege is that private browsing mode did not do what they (incorrectly) contend the Privacy Policy promised it would do, and thus their claim at best raises a "permission skirmish" that cannot trigger criminal liability. *Id.* at 1069.

Plaintiffs also argue (at 18) that the CCCL does not require circumvention of a barrier, contending that this Court's 2019 decision in *Brodsky* is inconsistent with the Ninth Circuit's 2015 decision in *U.S. v. Christensen*, 828 F.3d 763 (9th Cir. 2015). Not so. In *Christensen*, the Court merely held that the CCCL does not require "unauthorized access." 828 F.3d at 789 (the "term 'access' … includes logging into a database with a valid password" by a defendant who used his login credentials to steal data and sell it to a third party). The defendants in *Christensen* nevertheless overcame a "barrier"—*i.e.*, a password-protected login—by obtaining and using a valid password for an improper purpose. That is not the case here.

D. Plaintiffs' Privacy Claims (Counts 4-5) Do Not Meet the Standard in *Facebook*

Plaintiffs' arguments (at 22, 23) that their "expectation of privacy was even higher than in [*Facebook*]" and "Google's conduct is even more offensive than the conduct in [*Facebook*]," fall flat. A comparison of Plaintiffs' allegations to those in *Facebook* shows why their constitutional and common-law privacy claims should be dismissed.

No reasonable expectation of privacy. In *Facebook*, the Ninth Circuit held the plaintiffs alleged a reasonable expectation that their logged-out user data would not be collected by Facebook when they visited websites that used Facebook plugins *because* Facebook's disclosures "affirmatively stated" that "[i]f you log out of Facebook, *we will not receive this information*." 956

F.3d at 602. By contrast, Google's Privacy Policy discloses it *does* receive the Data "[w]hen *you're not signed in* to a Google Account." Ex. 8, at 2-4. In light of (i) this explicit disclosure; (ii) Plaintiffs' admission that it is "common knowledge that Google collects information about the web-browsing activity of users" (AC ¶ 163); and (iii) Plaintiffs' failure to identify an affirmative statement by Google that it would not receive the Data when a user is in private browsing mode, Plaintiffs fail to plausibly allege a reasonable expectation of privacy.

Moreover, unlike Facebook, which allegedly "compiled the referer headers it collected [from separate browsing sessions] into personal user profiles using 'cookies,'" 956 F.3d at 596, Google made clear that cookies set during an Incognito session *are deleted when the private browsing session is closed*, and thus the Data from separate logged-out private browsing sessions is not correlated into a user profile. Exs. 17, 18, 19. Plaintiffs incorrectly argue (at 9) that this aspect of Incognito mode is irrelevant. But "[t]he nature of the allegedly collected data is … important" to determine if a privacy claim has been pleaded. *Facebook*, 956 F.3d at 603. In *Facebook*, the data was "a comprehensive browsing history of an individual" because plaintiffs alleged that Facebook correlated individual URLs through appended "cookies that precisely identif[ied] the user" by "stor[ing] the user's login ID." *Id.* at 596, 603. Likewise, in *Google Cookie*, plaintiffs alleged that "the [i]nternet histories of users" were compiled with cookies and Google circumvented "cookie blockers." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 131, 150 (3d Cir. 2015). Without a similar plausible allegation here, the Data Google allegedly received is not individual users' browsing histories, but simply URLs not linked to any particular user, which cannot support Plaintiffs' state law invasion of privacy claims.

Plaintiffs alternatively argue that "Google associates the data with users' Google profiles," and assert that this generates a "factual dispute." Opp. 21 (citing AC ¶¶ 89-112). But not one of the paragraphs Plaintiffs cite states that Google compiles the Data from logged-out users' private browsing sessions in their Google accounts or in "profiles." Plaintiffs' vague citation to 23 paragraphs of the AC that purport to describe (albeit incorrectly) Google's *general* practices across its *many* products and services, does not help them. Google makes clear that it does not associate logged-out private browsing Data with "profiles," and the AC does not plausibly allege otherwise.

In light of Google's disclosures, Plaintiffs could reasonably have expected that (1) Google would not store Data from logged-out private browsing sessions in their accounts, and (2) that Chrome would delete any site data and cookies set during Incognito sessions when they closed the sessions. Plaintiffs fail to allege that Google acted inconsistently with such an expectation. And any expectation that private browsing mode would *prevent* Google from receiving the Data in the first place is not supported by the Privacy Policy or the other disclosures on which Plaintiffs rely.

No highly offensive conduct. The Motion demonstrates (at 21-22) that Plaintiffs fail to allege "highly offensive" conduct because (1) collection of browsing data not associated with a specific individual does not meet the standard, and (2) Google's receipt of the Data was "common knowledge" and served a legitimate commercial purpose. In response, Plaintiffs argue (at 22-23) that Google's cited authorities pre-date *Facebook,* which somehow negates their import. But *Facebook* itself supports the proposition that collecting or disclosing browsing history disassociated from a specific individual is not a "highly offensive" invasion of privacy. In *Facebook*, the Ninth Circuit held that plaintiffs pleaded a "highly offensive invasion" *because* they alleged that Facebook combined their logged-out user data with their logged-in user data—*and their Facebook profiles*—thereby "gain[ing] a cradle-to-grave profile without users' consent." *Facebook*, 956 F.3d at 599 ("Facebook's user profiles would allegedly reveal an *individual's* likes, dislikes, interests, and habits over a significant amount of time, without affording users a meaningful opportunity to control or prevent the unauthorized exploration of their private lives") (emphasis added). In contrast, Plaintiffs do not plausibly allege that Google links the Data to their identities, and thus fail to meet the standard. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1042 (N.D. Cal. 2014) (Koh, J) (dismissing privacy claim for failing to plead "serious invasion of privacy" where plaintiffs did not allege defendant "link[s] the information it acquires to Plaintiffs' *identities* (i.e., to their *names*) as opposed to just creating generic profiles that describe Plaintiffs' interests and general characteristics (female, likes shampoo products, etc).").

E. Plaintiffs' Claims Are Barred by the Statutes of Limitations

One week after Google filed its Motion, the Ninth Circuit held that, under the Wiretap Act, "each interception is a discrete violation" for statute of limitations purposes. *Bliss v. CoreCivic, Inc.*,

978 F.3d 1144, 1148 (9th Cir. 2020). Plaintiffs ask this Court (at 24) to rely on *Bliss* to rescue their untimely claims under CIPA, CDAFA, and for intrusion upon seclusion and violation of the California constitution, but the decision addressed none of those causes of action. At a minimum, there is no basis for applying this "logic" to Plaintiffs' state-law privacy claims.

In any event, Plaintiffs concede (at 24) that, to the extent they have stated a claim, it would be limited to "the statute-of-limitations period[s] prior to the filing of the original Complaint" (which are one, two, and three years),[10] and would not extend to the full four-year proposed Class Period unless a tolling doctrine applies (none do), and thus their claims should be limited accordingly.

Plaintiffs' reliance (at 24-25) on the fraudulent concealment and delayed discovery doctrines to toll their claims based on Google's conduct outside the limitations periods is misplaced. The AC fails to plausibly allege that: (1) Google fraudulently concealed that it receives the Data while users are in private browsing mode, *see supra* at I.A; and (2) Plaintiffs exercised reasonable diligence to discover their purported injuries. "[T]o merit application of the discovery rule or fraudulent concealment tolling, a plaintiff must allege that he exercised due diligence to uncover his injury." *Yetter v. Ford Motor Co.*, 428 F. Supp. 3d 210, 223 (N.D. Cal. 2019) (emphasis added); *Denholm v. Houghton Mifflin Co.*, 912 F.2d 357, 362 (9th Cir. 1990) ("It is imperative that the plaintiff plead in his complaint … the facts which excuse the plaintiff's failure to discover the [injury] sooner"). At best, Plaintiffs have alleged they misunderstood the Privacy Policy, which they could have clarified immediately by taking Google up on its offer on page 1 of the Privacy Policy to "contact us" "if you have any questions" about Google's practices. Ex. 1, at 1. Plaintiffs' failure to take this basic step—or to conduct any other diligence of their claims—precludes application of any tolling doctrines.

CONCLUSION

For the foregoing reasons, the Court should dismiss this action in its entirety with prejudice.

[10] Contrary to Plaintiffs' argument (at 25), the limitations period for CIPA is one year. *See Brodsky*, 445 F. Supp. 3d at 134; *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051 (N.D. Cal. 2018) (finding the statute of limitation for CIPA is one year under Cal. Code Civ. Pro. § 340(a)). The statute of limitations for invasion of privacy claims is also one year. *See Guilllen v. Bank of Am. Corp.*, 2011 WL 4071996, at *10 (N.D. Cal. Aug. 31, 2011).

DATED: December 7, 2020

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By */s/ Andrew H. Schapiro*

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Thao Thai (CA Bar No. 324672)
thaothai@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

William A. Burck (admitted *pro hac vice*)
williamburck@quinnemanuel.com
Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
1300 I. Street, N.W., Suite 900
Washington, D.C. 20005
Telephone: 202-538-8000
Facsimile: 202-538-8100

Jomaire A. Crawford (admitted *pro hac vice*)
jomairecrawford@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor

San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC